Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions

Ruoheng Liu, *Member, IEEE*, Ivana Marić, *Member, IEEE*, Predrag Spasojević, *Member, IEEE*, and Roy D. Yates *Member, IEEE*

Abstract*—We study information-theoretic security for discrete memoryless** *interference* **and** *broadcast* **channels with independent confidential messages sent to two receivers. Confidential messages are transmitted to their respective receivers with** *information-theoretic secrecy. That is, each receiver is kept in total ignorance with respect to the message intended for the other receiver. The secrecy level is measured by the equivocation rate at the eavesdropping receiver. In this paper, we present inner and outer bounds on secrecy capacity regions for these two communication systems. The derived outer bounds have an identical mutual information expression that applies to both channel models. The difference is in the input distributions over which the expression is optimized. The inner bound rate regions are achieved by** *random binning* **techniques. For the broadcast channel, a** *double-binning* **coding scheme allows for both joint encoding and preserving of confidentiality. Furthermore, we show that, for a special case of the interference channel, referred to as the** *switch* **channel, the two bound bounds meet. Finally, we describe several transmission schemes for Gaussian interference channels and derive their achievable rate regions while ensuring mutual information-theoretic secrecy. An encoding scheme in which transmitters dedicate some of their power to create** *artificial noise* **is proposed and shown to outperform both time-sharing and simple multiplexed transmission of the confidential messages.**

I. Introduction

The broadcast nature of a wireless medium allows for the transmitted signal to be received by all users within the communication range. Hence, wireless communication sessions are very susceptible to eavesdropping. The information-theoretic single user secure communication problem was first characterized using the *wiretap channel* model proposed by Wyner [1]. In this model, a single source-destination communication link is eavesdropped by a wiretapper via a degraded channel. The secrecy level is measured by the equivocation rate at the wiretapper. Wyner showed that secure communication is possible without sharing a secret key between legitimate users, and determined the tradeoff between the transmission rate and the secrecy level [1]. This result was generalized by Csiszár and Körner who determined the capacity region of the broadcast channel with confidential messages [2] in which a message intended for one of the receivers is confidential.

Following the work of Wyner [1] and Csiszár and Körner [2], the more recent information-theoretic research on secure communication focuses at implementing security on the physical layer. Based on independent efforts, the authors of [3] and [4] described achievable secure rate regions and outer bounds for a two-user discrete memoryless multiple access channel with confidential messages. This model generalizes the multiple access channel (MAC) [5, Sec. 14.3] by allowing each user (or one of the users) to receive noisy channel outputs and, hence, to eavesdrop the confidential information sent by the other user. In addition, the Gaussian MAC wiretap channel has been analyzed in [6]–[10]. The relay channel with confidential messages where the relay node acts as both a helper and a wiretapper has been considered in [11]. The relay-eavesdropper channel has been proposed in [12]. More recently, the cognitive interference channel with confidential messages has been addressed in [13]. The effects of fading on secure wireless communication have been studied in [14]–[18].

In this paper, we study two distinct but related in multi-terminal secure communication problems following the information-theoretic approach. We focus on discrete memoryless *interference* and *broadcast* channels with independent confidential messages sent to two receivers. Confidential messages are transmitted to their respective receivers while ensuring mutual *information-theoretic secrecy*. That is, each receiver is kept in total ignorance with respect to the message intended for the other receiver. We first derive outer bounds on capacity regions for these two communication systems. These bounds have an identical mutual information expression. The expression is optimized over different input distributions, i.e., for the interference channel, the two senders offer independent inputs to the channel and, for the broadcast channel, the sender jointly encodes both messages. We also derive achievable rate regions for the two channel models. Here, we only consider sending confidential messages and, hence, no common message in the sense of Marton [19] is conveyed to the receivers in the case of the broadcast channel. The inner bounds are achieved using *random binning* techniques. For the broadcast channel, a *double-binning* coding scheme which allows for

Manuscript received February 16, 2007; revised July 30, 2007 and October 15, 2007. This work was supported by NSF Grant ANI 0338805. The material in this paper was presented in part at the 44th Allerton Conference on Communication, Control, and Computing, Urbana, IL, USA, September, 2006 and Information Theory and Application Workshop (ITA), San Diego, CA, USA Jan-Feb, 2007.

R. Liu is with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (email: rliu@princeton.edu).

P. Spasojević and R. D. Yates are with WINLAB, Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ 08902 USA (email: {spasojev,ryates}@winlab.rutgers.edu).

I. Marić is with WSL, Department of Electrical Engineering, Stanford University, Stanford, CA 94305 (email: ivanam@wsl.stanford.edu).

both joint precoding as in the classical broadcast channel [19], and preserving of confidentiality. Similarly, ensuring of confidential messages precludes partial decoding of the message intended for the other receiver in the case of the interference channel. Hence, rate-splitting encoding used by Carleial [20] and Han and Kobayashi [21] employed with the classical interference channel is precluded. Instead, the encoders will use only stochastic encoders. We show that for the special case of the interference channel, referred to as the *switch* channel, derived bounds meet. Finally, we describe several transmission schemes for general Gaussian interference channels and derive their achievable rate regions while still ensuring information-theoretic secrecy. An encoding scheme in which transmitters dedicate some of their power to create *artificial noise* is proposed and shown to outperform both time-sharing and simple multiplexed transmission of the confidential messages.

The remainder of this paper is organized as follows. The notation and the channel model are given in Sec. II. We state the main results in Sec. III. Outer bounds are derived in Sec. IV. Inner bounds associated with the achievable coding scheme for the interference and broadcast channels with confidential messages are established in Sec. V. Finally, the results are summarized in Sec. VI.

II. Definitions and Notations

A. Notations

Throughout the paper, a random variable is denoted with an upper case letter (e.g., X), its realization is denoted with the corresponding lower case letter (e.g., x), the finite alphabet of the random variable is denoted with the corresponding calligraphic letter (e.g., $\mathcal{X}$), and its probability distribution is denoted with $P_X(x)$. For example, the random variable X with probability distribution $P(x) = P_X(x)$ takes on values in the finite alphabet $\mathcal{X}$. A boldface symbol denotes a sequence with the following conventions

$$\mathbf{X} = [X_1, \ldots, X_n], \quad \mathbf{X}^i = [X_1, \ldots, X_i],$$
$$\text{and} \quad \tilde{\mathbf{X}}^i = [X_i, \ldots, X_n].$$

Finally, we use $A_\epsilon^{(n)}(P_X)$ to denote the set of (weakly) jointly typical sequences $\mathbf{x}$ with respect to $P(x)$ (see [5] for more details).

B. The Interference Channel with Confidential Messages

Consider a discrete memoryless interference channel with finite input alphabets $\mathcal{X}_1$, $\mathcal{X}_2$, finite output alphabets $\mathcal{Y}_1$, $\mathcal{Y}_2$, and the channel transition probability distribution $P(y_1, y_2|x_1, x_2)$. Two transmitters wish to send independent, confidential messages to their respective receivers. We refer to such a channel as the *interference channel with confidential messages* (IC-CM). This communication model is shown in Fig. 1. Symbols $(x_1, x_2) \in (\mathcal{X}_1 \times \mathcal{X}_2)$ are the channel inputs at transmitters 1 and 2, and $(y_1, y_2) \in (\mathcal{Y}_1 \times \mathcal{Y}_2)$ are the channel outputs at receivers 1 and 2, respectively.

Transmitter t, $t = 1, 2$, intends to send an independent message $W_t \in \{1, \ldots, M_t\}$ to the desired receiver t in n channel uses while ensuring information-theoretic secrecy. The channel is memoryless in the sense that

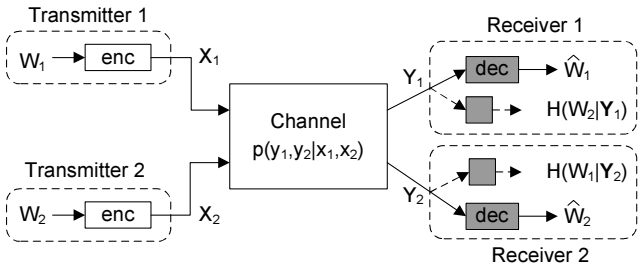


Fig. 1. Interference Channel with Confidential Messages.

$$P(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{n} P(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i}).$$

A stochastic encoder for transmitter t is described by a matrix of conditional probabilities $f_t(\mathbf{x}_t|w_t)$, where $\mathbf{x}_t \in \mathcal{X}_t^n$, $w_t \in \mathcal{W}_t$, and

$$\sum_{\mathbf{x}_t \in \mathcal{X}_t^n} f_t(\mathbf{x}_t|w_t) = 1.$$

Decoding functions are mappings $\psi_t : \mathcal{Y}_t \to \mathcal{W}_t$. Secrecy levels at receivers 1 and 2 are measured with respect to the equivocation rates

$$\frac{1}{n} H(W_2|\mathbf{Y}_1) \quad \text{and} \quad \frac{1}{n} H(W_1|\mathbf{Y}_2). \tag{1}$$

An $(M_1, M_2, n, P_e^{(n)})$ code for the interference channel consists of two encoding functions f_1, f_2, two decoding functions ψ_1, ψ_2, and the corresponding maximum average error probability

$$P_e^{(n)} \triangleq \max\{P_{e,1}^{(n)}, P_{e,2}^{(n)}\} \tag{2}$$

where, for $t = 1, 2$,

$$P_{e,t}^{(n)} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} P\big[\psi_t(\mathbf{Y}_t) \neq w_t | (w_1, w_2) \text{ sent}\big].$$

A rate pair (R_1, R_2) is said to be *achievable* for the interference channel with confidential messages if, for any $\epsilon_0 > 0$, there exists a $(M_1, M_2, n, P_e^{(n)})$ code such that

$$M_t \geq 2^{nR_t} \quad \text{for } t = 1, 2 \tag{3}$$

and the reliability requirement

$$P_e^{(n)} \leq \epsilon_0 \tag{4}$$

and the security constraints

$$nR_1 - H(W_1|\mathbf{Y}_2) \leq n\epsilon_0 \tag{5a}$$
$$nR_2 - H(W_2|\mathbf{Y}_1) \leq n\epsilon_0 \tag{5b}$$

are satisfied. This definition corresponds to the so-called *weak secrecy-key rate* [22]. A stronger measurement of the secrecy level has been defined by Maurer and Wolf in terms of the absolute equivocation [22], where the authors have shown that the former definition could be replaced by the latter without any rate penalty for the wiretap channel.

The capacity region of the IC-CM is the closure of the set of all achievable rate pairs (R_1, R_2), denoted by $\mathbb{C}_{\text{IC}}$.

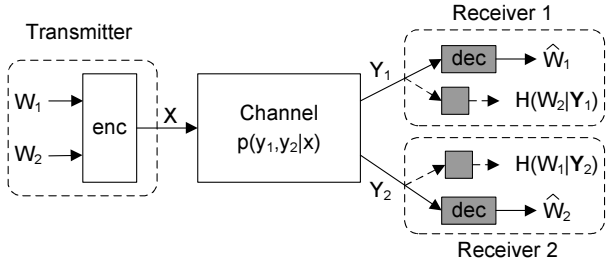


Fig. 2. Broadcast Channel with Confidential Messages.

C. The Broadcast Channel

We also consider the *broadcast channel with confidential messages* (BC-CM) in which secret messages from a single transmitter are to be communicated to two receivers, as shown in Fig. 2. A discrete memoryless BC-CM is described using finite sets $\mathcal{X}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$, and a conditional probability distribution $P(y_1, y_2|x)$. Symbols $x \in \mathcal{X}$ are channel inputs and $(y_1, y_2) \in (\mathcal{Y}_1 \times \mathcal{Y}_2)$ are channel outputs at receivers 1 and 2, respectively. The transmitter intends to send an independent message $W_t \in \{1, \ldots, M_t\} \triangleq \mathcal{W}_t$ to the respective receiver $t \in \{1, 2\}$ in n channel uses while ensuring information-theoretic secrecy as given by (5a) and (5b). The channel is memoryless in the sense that

$$P(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}) = \prod_{i=1}^{n} P(y_{1,i}, y_{2,i}|x_i).$$

A stochastic encoder is specified by a matrix of conditional probabilities $f(\mathbf{x}|w_1, w_2)$, where $\mathbf{x} \in \mathcal{X}^n$, $w_t \in \mathcal{W}_t$, and

$$\sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|w_1, w_2) = 1.$$

Note that $f(\mathbf{x}|w_1, w_2)$ is the probability that the pair of messages (w_1, w_2) are encoded as the channel input $\mathbf{x}$. The decoding function at the receiver t is a mapping $\phi_t : \mathcal{Y}_t \to \mathcal{W}_t$.

The secrecy levels of confidential messages W_2 and W_1 are measured, respectively, at receivers 1 and 2 in terms of the equivocation rates (1). An $(M_1, M_2, n, P_e^{(n)})$ code for the broadcast channel consists of the encoding function f, decoding functions ϕ_1, ϕ_2, and the maximum error probability $P_e^{(n)}$ in (2), where, for $t = 1, 2$,

$$P_{e,t}^{(n)} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} P\big[\phi_t(\mathbf{Y}_t) \neq w_t | (w_1, w_2) \text{ sent}\big]. \quad (6)$$

A rate pair (R_1, R_2) is said to be achievable for the broadcast channel with confidential messages if, for any $\epsilon_0 > 0$, there exists a $(M_1, M_2, n, P_e^{(n)})$ code which satisfies (3)–(5).

The capacity region of the BC-CM is the closure of the set of all achievable rate pairs (R_1, R_2), denoted by $\mathbb{C}_{\rm BC}$.

III. Main Results

In this section, we state our main results. We first describe the outer and inner bounds on the capacity regions of both interference and broadcast channels with confidential messages. We then show that the derived bounds meet for a special case of the interference channel, called the switch channel. Finally, we propose several transmission schemes for Gaussian interference channels and derive their achievable rate regions under information-theoretic secrecy.

A. Interference Channel with Confidential Messages

Let U, V_1, and V_2 be auxiliary random variables. We consider the following two classes of joint distributions for the interference channel. Let $\pi_{\rm IC-O}$ be the class of distributions $P(u, v_1, v_2, x_1, x_2, y_1, y_2)$ that factor as

$$P(u)P(v_1, v_2|u)P(x_1|v_1)P(x_2|v_2)P(y_1, y_2|x_1, x_2), \quad (7)$$

and $\pi_{\rm IC-I}$ be the class of distributions that factor as

$$P(u)P(v_1|u)P(v_2|u)P(x_1|v_1)P(x_2|v_2)P(y_1, y_2|x_1, x_2). \quad (8)$$

Theorem 1: [outer bound for IC-CM] Let $\mathbb{R}_{\rm O}(\pi_{\rm IC-O})$ denote the union of all (R_1, R_2) satisfying

$$0 \le R_1 \le \min \left[\begin{array}{l} I(V_1; Y_1|U) - I(V_1; Y_2|U), \\ I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U) \end{array} \right] \quad (9a)$$

$$0 \le R_2 \le \min \left[\begin{array}{l} I(V_2; Y_2|U) - I(V_2; Y_1|U), \\ I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U) \end{array} \right] \quad (9b)$$

over all distributions $P(u, v_1, v_2, x_1, x_2, y_1, y_2)$ in $\pi_{\rm IC-O}$. For the interference channel $(\mathcal{X}_1 \times \mathcal{X}_2, P(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with confidential messages, the capacity region

$$\mathbb{C}_{\rm IC} \subseteq \mathbb{R}_{\rm O}(\pi_{\rm IC-O}).$$

Proof: We provide the proof of Theorem 1 in Sec. IV. ■

Theorem 2: [inner bound for IC-CM] Let $\mathbb{R}_{\rm IC}(\pi_{\rm IC-I})$ denote the union of all (R_1, R_2) satisfying

$$0 \le R_1 \le I(V_1; Y_1|U) - I(V_1; Y_2|V_2, U) \quad (10a)$$

$$0 \le R_2 \le I(V_2; Y_2|U) - I(V_2; Y_1|V_1, U) \quad (10b)$$

over all distributions $P(u, v_1, v_2, x_1, x_2, y_1, y_2)$ in $\pi_{\rm IC-I}$. Any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\rm IC}(\pi_{\rm IC-I})$$

is achievable for the interference channel with confidential messages.

Proof: We provide the proof in Sec. V-A. ■

To derive the achievable rate region for the IC-CM, we employ an auxiliary random variable U in the sense of Han-Kobayashi [21]. For a given U, we consider two independent stochastic encoders, that is, the pre-coding auxiliary random variables V_1 and V_2 will be independent for a given U, as given by (8). To ensure information-theoretic secrecy, the achievable rate R_1 includes a penalty term $I(V_1; Y_2|V_2, U)$, which is a conditional mutual information of the receiver 2's eavesdropper channel while assuming the receiver 2 can first decode its own information.

B. Broadcast Channel with Confidential Messages

For the broadcast channel, we focus on the class of distributions $P(u, v_1, v_2, x, y_1, y_2)$ that factor as

$$P(u)P(v_1, v_2|u)P(x|v_1, v_2)P(y_1, y_2|x). \quad (11)$$

We refer to this class as $\pi_{\rm BC}$.

Theorem 3: [outer bound for BC-CM] Let $\mathbb{R}_{\rm O}(\pi_{\rm BC})$ denote the union of all (R_1, R_2) satisfying

$$R_1 \geq 0,\ R_2 \geq 0$$
$$R_1 \leq \min \left[\begin{array}{l} I(V_1;Y_1|U) - I(V_1;Y_2|U), \\ I(V_1;Y_1|V_2,U) - I(V_1;Y_2|V_2,U) \end{array} \right] \quad (12a)$$
$$R_2 \leq \min \left[\begin{array}{l} I(V_2;Y_2|U) - I(V_2;Y_1|U), \\ I(V_2;Y_2|V_1,U) - I(V_2;Y_1|V_1,U) \end{array} \right] \quad (12b)$$

over all distributions $P(u, v_1, v_2, x, y_1, y_2)$ in $\pi_{\rm BC}$ and auxiliary random variables U, V_1, and V_2 satisfying

$$U \to V_1 \to X \quad \text{and} \quad U \to V_2 \to X. \quad (13)$$

For the broadcast channel $(\mathcal{X}, P(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with confidential messages, the capacity region

$$\mathbb{C}_{\rm BC} \subseteq \mathbb{R}_{\rm O}(\pi_{\rm BC}).$$

Proof: We provide the proof of Theorem 3 in Sec. IV. ■

Remark 1: Outer bounds for the BC-CM and the IC-CM have a same mutual information expression $\mathbb{R}_{\rm O}(\cdot)$, but, they are optimized over different input distributions $\pi_{\rm BC}$ and $\pi_{\rm IC-O}$, respectively.

Theorem 4: [inner bound for BC-CM] Let $\mathbb{R}_{\rm BC}(\pi_{\rm BC})$ denote the union of all (R_1, R_2) satisfying

$$R_1 \geq 0,\ R_2 \geq 0$$
$$R_1 \leq I(V_1;Y_1|U) - I(V_1;V_2|U) - I(V_1;Y_2|V_2,U) \quad (14a)$$
$$R_2 \leq I(V_2;Y_2|U) - I(V_1;V_2|U) - I(V_2;Y_1|V_1,U) \quad (14b)$$

over all distributions $P(u, v_1, v_2, x, y_1, y_2)$ in $\pi_{\rm BC}$. Any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\rm BC}(\pi_{\rm BC})$$

is achievable for the broadcast channel with confidential messages.

Proof: We provide the proof in Sec. V-B. ■

We note that, for a broadcast channel, we can employ joint encoding at the transmitter. Hence, the achievable coding scheme for the BC-CM is based on the *double-binning* scheme which combines the *Gel'fand-Pinsker binning* [23] and the *random binning*. To preserve confidentiality, the achievability bounds on R_1 and R_2 each include the penalty term $I(V_1;V_2|U)$. Without the confidentiality constraint, Marton's inner bound [19] on the broadcast channel illustrates only that the sum rate has the penalty term $I(V_1;V_2|U)$. To ensure information-theoretic secrecy, the proposed coding scheme pays "double" when jointly encoding at the transmitter.

Example 1: [less noisy broadcast channel] Consider a special class of broadcast channels in which the channel $X \to Y_1$ is *less noisy* than the channel $X \to Y_2$, i.e.,

$$I(V;Y_1) \geq I(V;Y_2) \quad (15)$$

for every $V \to X \to (Y_1, Y_2)$ [2]. We first consider the outer bound of the less noisy BC-CM. Based on the Markov chains in (13) and the definition (15), we have

$$I(V_1;Y_1|U=u) \geq I(V_1;Y_2|U=u)$$
$$I(V_2;Y_1|U=u) \geq I(V_2;Y_2|U=u),$$

which implies that

$$I(V_1;Y_1|U) \geq I(V_1;Y_2|U)$$
$$I(V_2;Y_1|U) \geq I(V_2;Y_2|U).$$

Hence the outer bound can be rewritten as the union of all (R_1, R_2) satisfying

$$R_1 \leq \max_{P(X)} [I(X;Y_1) - I(X;Y_2)] \quad (16a)$$
$$R_2 = 0 \quad (16b)$$

where (16a) follows from [2, Theorem 3]. Next, by applying Theorem 4 and setting $V_2 = U =$ const, we obtain the identical rate region as (16). This result implies that only the "better" user can get the non-zero secrecy rate for the less noisy BC-CM. Note that, the single-antenna Gaussian broadcast channel is a special case of the less noisy broadcast channel.

In the following, we consider a sufficient condition under which both R_1 and R_2 can be strictly positive for the BC-CM.

Corollary 1: For a broadcast channel, if there exist a distribution $P(u, v_1, v_2, x, y_1, y_2) \in \pi_{\rm BC}$ for which

$$I(V_1;Y_1|U) > I(V_1;Y_2,V_2|U) \quad (17a)$$
$$\text{and} \qquad I(V_2;Y_2|U) > I(V_2;Y_1,V_1|U), \quad (17b)$$

then both receivers can achieve strictly positive rates while ensuring information-theoretic secrecy.

Proof: The result is obtained by applying Theorem 4 and by setting $R_1 > 0$ and $R_2 > 0$. ■

More recently, motivated by this work, the multiple-antenna Gaussian broadcast channel with confidential messages was studied in [24]. It was shown that with multiple antennas at transmitters, strictly positive rates to both receivers can be achieved while ensuring information-theoretic secrecy.

C. Switch Channel

In this subsection, we obtain the secrecy capacity region for a special case of the interference channel referred to as the switch channel (SC). As shown in Fig. 3, receivers in the SC cannot listen to both transmissions (from encoders 1 and 2) at the same time. For example, each encoder may transmit at a different frequency, while each receiver may listen only to one frequency during each symbol time i. We assume that each receiver $t \in \{1, 2\}$ has a random switch $s_t \in \{1, 2\}$, which chooses between t and $\bar{t}$ independently at each symbol time i with probabilities

$$P(S_{t,i} = t) = \tau_t$$
$$P(S_{t,i} = \bar{t}) = 1 - \tau_t, \quad i = 1, \ldots, n$$

where $\bar{t}$ is the complement of t. Therefore, receiver t listens to its own information $x_{t,i}$ from encoder t whenever $S_{t,i} = t$, while it eavesdrops the signal $x_{\bar{t},i}$ when $S_{t,i} = \bar{t}$. By assuming that the switch state information is available at the receiver, we have that

$$\begin{aligned} P(y_{t,i}|x_{1,i}, x_{2,i}, s_{t,i}) &= P(y_{t,i}|x_{1,i})\mathbf{1}(s_{t,i} = 1) \\ &\quad + P(y_{t,i}|x_{2,i})\mathbf{1}(s_{t,i} = 2) \\ &= P(y_{t,i}|x_{s_{t,i},i}) \end{aligned} \quad (18)$$

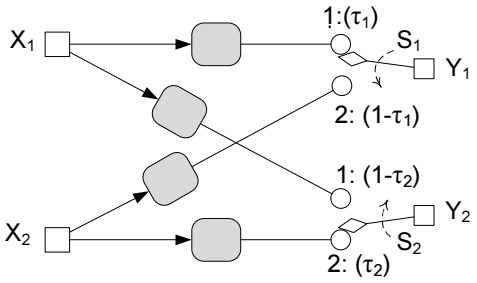


Fig. 3. Switch channel model

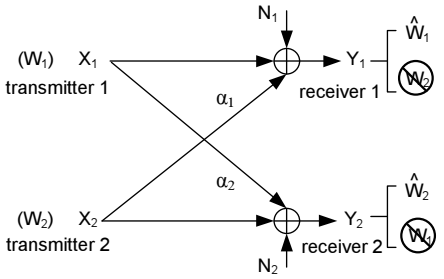


Fig. 4. Gaussian interference channel with confidential messages

where $\mathbf{1}(\cdot)$ is the indicator function.

The switch state information $\{S_{t,i}\}_{i=1}^{n}$ is an i.i.d. process known at receiver t. Hence, we can consider $s_{t,i}$ as a part of the channel output, i.e., we set

$$y_{t,i} \triangleq \{z_{t,i},\ s_{t,i}\} \tag{19}$$

where $z_{t,i}$ represents the received signal value at receiver t. Under this setting, we have the following theorem on the secrecy capacity region $\mathbb{C}_{\rm SC}$ of SC-CM.

Theorem 5: For the switch channel with confidential messages, the capacity region $\mathbb{C}_{\rm SC}$ is the union of all (R_1, R_2) satisfying

$$0 \le R_1 \le I(V_1; Y_1|U) - I(V_1; Y_2|V_2, U) \tag{20a}$$
$$0 \le R_2 \le I(V_2; Y_2|U) - I(V_2; Y_1|V_1, U) \tag{20b}$$

over all distributions $P(u, v_1, v_2, x_1, x_2, y_1, y_2)$ in $\pi_{\rm IC-I}$.

Proof: We provide the proof in the Appendix. ■

Remark 2: In SC-CM, receiver t listens to the desired information during time fraction τ_t, and intercepts the other message during the time fraction $(1-\tau_t)$. When $\tau_1 = \tau_2 = 1$, both receivers only listen to their own messages and thus SC-CM reduces to two independent parallel channels without the secrecy constraints. When $\tau_1 = 1$ and $\tau_2 = 0$, receiver 2 acts as an eavesdropper only and both Y_1 and Y_2 are independent with respect to the message W_2. Hence, in this case, SC-CM reduces to the wiretap channel [1].

Example 2: [noiseless memoryless switch channel] We assume that the channel is discrete memoryless and that the input-output relationship at each time instant satisfies

$$Y_{t,i} = \begin{cases} X_{1,i}, & S_{t,i} = 1 \\ X_{2,i}, & S_{t,i} = 2 \end{cases} \qquad \text{for} \quad i = 1, \ldots, n \tag{21}$$

where $P(S_{t,i} = t) = \tau_t$ and $\tau_1 + \tau_2 \ge 1$. Theorem 5 implies that the secrecy capacity region of this channel is:

$$\left\{ (R_1, R_2) : \begin{array}{l} R_1 \le (\tau_1 + \tau_2 - 1) H(X_1) \\ R_2 \le (\tau_1 + \tau_2 - 1) H(X_2) \end{array} \right\}. \tag{22}$$

We note that here $\tau_1 + \tau_2 - 1$ equals $\tau_1 - (1 - \tau_2)$, the time that user 1 sends without user 2 listening and also equals $\tau_2 - (1 - \tau_1)$, the time that user 2 sends without user 1 listening.

D. Gaussian Interference Channel with Confidential Messages

We next consider a Gaussian interference channel (GIC) with confidential messages (GIC-CM) where each node employs a single antenna as shown in Fig. 4. We have proposed this problem originally in [25].

We assume the channel input and output symbols to be from an alphabet of real numbers. Following the standard form GIC [20], the received symbols are

$$Y_1 = X_1 + \alpha_1 X_2 + N_1 \tag{23a}$$
$$Y_2 = \alpha_2 X_1 + X_2 + N_2 \tag{23b}$$

where α_1 and α_2 are normalized crossover *channel gains*, X_1 and X_2 are transmitted symbols from encoders 1 and 2 with the average power constraint

$$\sum_{i=1}^{n} \frac{\mathsf{E}[X_{t,i}^2]}{n} \le P_t, \quad \text{for } t = 1, 2,$$

and N_1 and N_2 correspond to two independent, zero-mean, unit-variance, Gaussian noise variables. In the following, we focus on the *weak* interference channel, i.e., $0 \le \alpha_1^2 < 1$ and $0 \le \alpha_2^2 < 1$. We describe three transmission schemes and their achievable rate regions under the requirement of information-theoretic secrecy.

1) Time-Sharing: The transmission period is divided into two non-overlapping slots with time fractions ρ_1 and ρ_2, where $\rho_1 \ge 0$, $\rho_2 \ge 0$, and $\rho_1 + \rho_2 = 1$. Transmitter t sends confidential message W_t in slot t with time fraction ρ_t, $t = 1, 2$. We refer to this technique as the time-sharing scheme. We note that, in each slot, the channel reduces to a Gaussian wiretap channel [26]. Let $\mathbb{R}_{\rm GIC}^{[\rm T]}$ denote the set of (R_1, R_2) satisfying

$$0 \le R_1 \le \frac{\rho_1}{2}\left[\log\left(1 + \frac{P_1}{\rho_1}\right) - \log\left(1 + \alpha_2^2 \frac{P_1}{\rho_1}\right)\right]$$
$$0 \le R_2 \le \frac{\rho_2}{2}\left[\log\left(1 + \frac{P_2}{\rho_2}\right) - \log\left(1 + \alpha_1^2 \frac{P_2}{\rho_2}\right)\right]$$

over all time fractions (ρ_1, ρ_2) pairs. Following [26], we can show that any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\rm GIC}^{[\rm T]}$$

is achievable for GIC-CM.

2) Multiplexed Transmission: In the multiplexed transmission scheme, we allow communication links to share the same degrees of freedom. Since we require information-theoretic secrecy for confidential messages, no partial decoding of the other transmitter's message is allowed at a receiver. Hence, the interference results in an increase of the noise floor. Let

$$0 \le \beta_t \le 1, \quad t = 1, 2.$$

By independently choosing

$$V_t = X_t \sim \mathcal{N}[0, \beta_t P_t], \quad t = 1, 2$$

and letting U serve as a convex combination operator, Theorem 2 implies that any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{M}]}$$

is achievable for GIC-CM, where $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{M}]}$ denotes the convex hull of the set of (R_1, R_2) satisfying

$$\begin{aligned} &R_1 \geq 0, \quad R_2 \geq 0 \\ &R_1 \leq \frac{1}{2}\log\left(1 + \frac{\beta_1 P_1}{1 + \alpha_1^2 \beta_2 P_2}\right) - \frac{1}{2}\log(1 + \alpha_2^2 \beta_1 P_1) \\ &R_2 \leq \frac{1}{2}\log\left(1 + \frac{\beta_2 P_2}{1 + \alpha_2^2 \beta_1 P_1}\right) - \frac{1}{2}\log(1 + \alpha_1^2 \beta_2 P_2) \end{aligned}$$

over all power-control parameters β_1 and β_2.

3) Artificial Noise: We next describe a scheme which allows one of the transmitters (e.g., transmitter 2) to generate artificial noise. This strategy involves splitting of the transmission power of transmitter 2 into two parts $P_{2,M}$ and $P_{2,A}$, where

$$\begin{aligned} P_{2,M} &= (1 - \lambda)\beta_2 P_2, \\ P_{2,A} &= \lambda \beta_2 P_2, \quad \text{and} \quad 0 \leq \lambda \leq 1, \end{aligned}$$

so that transmitter 2 encodes the confidential message with power $P_{2,M}$ and generates artificial noise with power $P_{2,A}$. The artificial noise can spoil the received signal of receiver 2 and, hence, protect the confidential message of transmitter 1. In this sense, this scheme allows *transmitter cooperation* without exchanging confidential messages. Let U serve as a convex combination operator,

$$X_1 = V_1 \quad \text{and} \quad X_2 = V_2 + A_2 \tag{26}$$

where V_1, V_2, and A_2 are independent Gaussian random variables:

$$\begin{aligned} V_1 &\sim \mathcal{N}[0, \beta_1 P_1], \\ V_2 &\sim \mathcal{N}[0, P_{2,M}], \\ \text{and} \qquad A_2 &\sim \mathcal{N}[0, P_{2,A}]. \end{aligned}$$

Here A_2 denotes the artificial noise which cannot be predicted and subtracted by either receiver. Since

$$\begin{aligned} Y_1 &= X_1 + \alpha_1 X_2 + N_1 \\ &= V_1 + \alpha_1(V_2 + A_2) + N_1 \end{aligned}$$

and

$$\begin{aligned} Y_2 &= \alpha_2 X_1 + X_2 + N_1 \\ &= \alpha_2 V_1 + (V_2 + A_2) + N_2, \end{aligned}$$

we have

$$\begin{aligned} I(V_1; Y_1) &= I(V_1;\, V_1 + \alpha_1(V_2 + A_2) + N_1) \\ &= h(V_1 + \alpha_1(V_2 + A_2) + N_1) \\ &\quad - h(\alpha_1(V_2 + A_2) + N_1) \\ &= \frac{1}{2}\log\left(1 + \frac{\beta_1 P_1}{1 + \alpha_1^2 \beta_2 P_2}\right) \end{aligned}$$

and

$$\begin{aligned} I(V_1; Y_2|V_2) &= I(V_1;\, \alpha_2 V_1 + V_2 + A_2 + N_2|V_2) \\ &= h(\alpha_2 V_1 + A_2 + N_2) - h(A_2 + N_2) \\ &= \frac{1}{2}\log\left(1 + \frac{\alpha_2^2 \beta_1 P_1}{1 + \lambda \beta_2 P_2}\right). \end{aligned}$$

Similarly, we can calculate

$$I(V_2; Y_2) = \frac{1}{2}\log\left[1 + \frac{(1 - \lambda)\beta_2 P_2}{1 + \alpha_2^2 \beta_1 P_1 + \lambda \beta_2 P_2}\right]$$

and

$$I(V_2; Y_1|V_1) = \frac{1}{2}\log\left[1 + \frac{(1 - \lambda)\alpha_1^2 \beta_2 P_2}{1 + \lambda \alpha_1^2 \beta_2 P_2}\right].$$

Applying Theorem 2, we can prove that any rate pair

$$(R_1, R_2) \in \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{A}]}$$

is achievable for GIC-CM, where $\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{A}]}$ denotes the convex hull of the set of (R_1, R_2) satisfying

$$\begin{aligned} 0 \leq R_1 \leq{}& \frac{1}{2}\log\left(1 + \frac{\beta_1 P_1}{1 + \alpha_1^2 \beta_2 P_2}\right) \\ &- \frac{1}{2}\log\left(1 + \frac{\alpha_2^2 \beta_1 P_1}{1 + \lambda \beta_2 P_2}\right) \qquad (27a) \\ 0 \leq R_2 \leq{}& \frac{1}{2}\log\left[1 + \frac{(1 - \lambda)\beta_2 P_2}{1 + \alpha_2^2 \beta_1 P_1 + \lambda \beta_2 P_2}\right] \\ &- \frac{1}{2}\log\left[1 + \frac{(1 - \lambda)\alpha_1^2 \beta_2 P_2}{1 + \lambda \alpha_1^2 \beta_2 P_2}\right] \qquad (27b) \end{aligned}$$

over all power-control parameter pair (β_1, β_2) and the power-splitting parameter λ. Furthermore, the achievable region can be increased by reversing the roles of transmitters 1 and 2.

Remark 3: We note that secure communication in a Gaussian channel with two senders and two receivers was also considered in [9], [10] for the Gaussian MAC with a wire-tapper (GMAC-WT). In this setting, both messages are to be conveyed to one of the receivers and none to the other receiver. Although the two problem formulations differ, the absence of rate splitting in the interference channel results in that the two proposed encoding schemes have a closer relationship than the schemes suggested for the classical MAC and interference channels. In fact, the encoding scheme proposed in [9], [10] for the GMAC-WT, referred to as *cooperative jamming*, and our encoding scheme which creates *artificial noise* in (26) are the same.

Example 3: In Fig. 5, we compare the achievable regions:

$$\mathbb{R}_{\mathrm{GIC}}^{[\mathrm{T}]}, \ \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{M}]}, \text{ and } \mathbb{R}_{\mathrm{GIC}}^{[\mathrm{A}]}$$

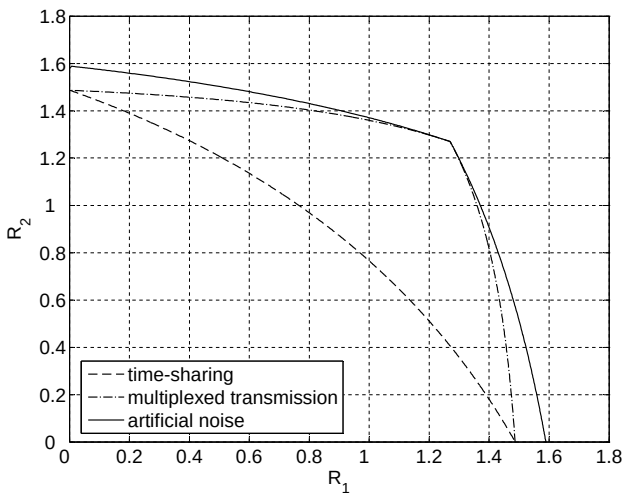
by numerical calculation, for

$$P_1 = P_2 = 10 \text{ and } \alpha_1 = \alpha_2 = 0.2$$

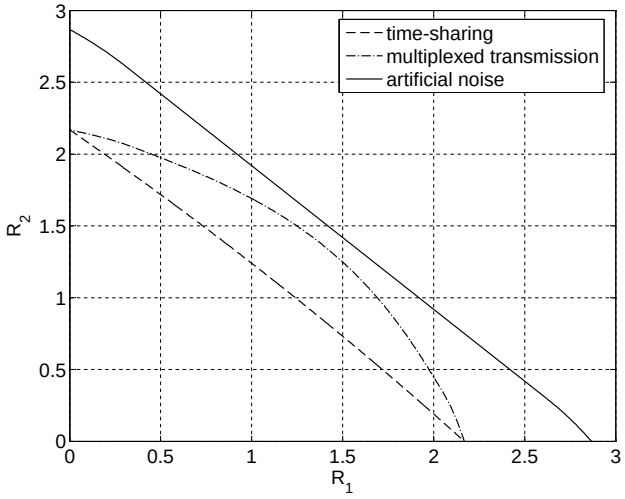
in Fig. 5.a and

$$P_1 = P_2 = 100 \text{ and } \alpha_1 = \alpha_2 = 0.2$$

in Fig. 5.b. Both numerical results illustrate that the artificial noise strategy allows for communication over larger rates, when compared to the time-sharing and multiplexed transmission schemes.



a. $P_1 = P_2 = 10$



a. $P_1 = P_2 = 100$

Fig. 5. Achievability regions for the GIC-CM ($\alpha_1 = \alpha_2 = 0.2$).

IV. Outer Bound

In this section we prove Theorems 1 and 3. In the following, we derive the upper bound for R_1. The upper bound for R_2 follows by symmetry.

The basis for the outer bound derivation is the reliable transmission requirement and the security constraint. Based on Fano's inequality [5], the reliable transmission requirement (4) implies that

$$H(W_1|\mathbf{Y}_1) \le \epsilon_0 \log(M_1 - 1) + h(\epsilon_0) \triangleq n\delta_1. \quad (28a)$$

$$H(W_2|\mathbf{Y}_2) \le \epsilon_0 \log(M_2 - 1) + h(\epsilon_0) \triangleq n\delta_2. \quad (28b)$$

where $h(x)$ is the binary entropy function. On the other hand, the security constraint (5a) implies that

$$nR_1 = H(W_1) \le H(W_1|\mathbf{Y}_2) + n\epsilon_0. \quad (29)$$

In fact, the bound (9) on R_1 is based on the following two different upper bounds on the equivocation $H(W_1|\mathbf{Y}_2)$.

A. First Bound

The first upper bound is derived by applying the techniques in [2]. By using Fano's inequality (28a), we obtain the following bound on the equivocation

$$H(W_1|\mathbf{Y}_2) \le H(W_1|\mathbf{Y}_2) - H(W_1|\mathbf{Y}_1) + n\delta_1. \quad (30)$$

Let

$$U_i = (\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}). \quad (31)$$

Since $(U_i, Y_{2,i}) = (\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i}) = (U_{i-1}, Y_{1,i-1})$, we have

$$H(W_1|U_i, Y_{2,i}) - H(W_1|U_{i-1}, Y_{1,i-1}) = 0$$

and we can rewrite (30) as follows

$$\begin{aligned} H(W_1|\mathbf{Y}_2) &\le H(W_1|\mathbf{Y}_2) - H(W_1|\mathbf{Y}_1) \\ &\quad + \sum_{i=2}^{n} \big[H(W_1|U_i, Y_{2,i}) \\ &\quad - H(W_1|U_{i-1}, Y_{1,i-1})\big] + n\delta_1. \end{aligned} \quad (32)$$

Note that

$$\mathbf{Y}_1 = (U_n, Y_{1,n}) \quad \text{and} \quad \mathbf{Y}_2 = (U_1, Y_{2,1}).$$

Hence, the bound (32) can be expressed as follows

$$\begin{aligned} &H(W_1|\mathbf{Y}_2) \\ &\quad \le H(W_1|U_1, Y_{2,1}) - H(W_1|U_n, Y_{1,n}) \\ &\qquad + \sum_{i=2}^{n} H(W_1|U_i, Y_{2,i}) - \sum_{i=1}^{n-1} H(W_1|U_i, Y_{1,i}) + n\delta_1 \\ &\quad = \sum_{i=1}^{n} [H(W_1|U_i, Y_{2,i}) - H(W_1|U_i, Y_{1,i})] + n\delta_1 \\ &\quad = \sum_{i=1}^{n} [I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i)] + n\delta_1 \ . \end{aligned} \quad (33)$$

Inequalities (29) and (33) imply that

$$nR_1 - n(\delta_1 + \epsilon_0) \le \sum_{i=1}^{n} [I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i)].$$

Now, for $\delta \triangleq \delta_1 + \epsilon_0$, we have

$$R_1 \le \frac{1}{n} \sum_{i=1}^{n} [I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i)] + \delta. \quad (34)$$

Following [5, Chapter 14], we introduce a random variable Q uniformly distributed over $\{1, 2, \ldots, n\}$ and independent of $(W_1, W_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}_1, \mathbf{Y}_2)$. Now we can bound R_1 as follows

$$\begin{aligned} R_1 &\le \frac{1}{n} \sum_{i=1}^{n} [I(W_1; Y_{1,i}|U_i, Q = i) \\ &\qquad - I(W_1; Y_{2,i}|U_i, Q = i)] + \delta \\ &= \sum_{i=1}^{n} P(Q = i)[I(W_1; Y_{1,Q}|U_Q, Q = i) \\ &\qquad - I(W_1; Y_{2,Q}|\mathbf{Y}_1^{Q-1}, \tilde{\mathbf{Y}}_2^{Q+1}, Q = i)] + \delta \\ &= I(W_1; Y_{1,Q}|U_Q, Q) - I(W_1; Y_{2,Q}|U_Q, Q) + \delta. \end{aligned} \quad (35)$$

Let

$$U \triangleq (U_Q, Q), \quad X_1 \triangleq X_{1,Q}, \quad X_2 \triangleq X_{2,Q},$$
$$Y_1 \triangleq Y_{1,Q}, \quad Y_2 \triangleq Y_{2,Q},$$
$$V_1 \triangleq (W_1, U), \quad V_2 \triangleq (W_2, U). \tag{36}$$

Note that, under the setting (36), the conditional distribution of $P(y_1, y_2|x_1, x_2)$ coincides with the original channel transition probability. We can rewrite (35) as

$$R_1 \leq I(V_1; Y_1|U) - I(V_1; Y_2|U) + \delta. \tag{37}$$

Remark 4: Note that we employ only Fano's inequality (28a) to derive the first bound on R_1.

B. Second Bound

The basic idea of the second bound can be described as follows. We assume that a genie gives receiver 1 message W_2, while receiver 2 attempts to evaluate the equivocation with W_2 as side information.

Now, the equivocation can be upper bounded by

$$\begin{aligned} H(W_1|\mathbf{Y}_2) &\leq H(W_1, W_2|\mathbf{Y}_2) \\ &= H(W_1|\mathbf{Y}_2, W_2) + H(W_2|\mathbf{Y}_2). \end{aligned} \tag{38}$$

By applying (28a) and (28b), we have

$$H(W_1|\mathbf{Y}_1) \leq n\delta_1 \quad \text{and} \quad H(W_2|\mathbf{Y}_2) \leq n\delta_2. \tag{39}$$

Since $H(W_1|\mathbf{Y}_1, W_2) \leq H(W_1|\mathbf{Y}_1)$, we can further bound (38) as follows

$$\begin{aligned} H(W_1|\mathbf{Y}_2) &\leq H(W_1|\mathbf{Y}_2, W_2) + n\delta_2 \\ &\leq H(W_1|\mathbf{Y}_2, W_2) - H(W_1|\mathbf{Y}_1, W_2) \\ &\quad + n(\delta_1 + \delta_2). \end{aligned} \tag{40}$$

Let $\delta' = \delta_1 + \delta_2 + \epsilon_0$. Following the same approach as in (30)–(36), we obtain

$$R_1 \leq I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U) + \delta'. \tag{41}$$

Remark 5: In order to get the second bound on R_1, we employ the requirement that not only receiver 1 can decode the message W_1 successfully, but also receiver 2 can decode the message W_2 successfully in (39) and (40) and, hence, we use Fano's inequalities (28a) and (28b).

C. Outer Bound and Discussion

Combining the two upper bounds (37) with (41) and assuming that δ and δ' converge to 0, we have

$$R_1 \leq \min \left[\begin{array}{l} I(V_1; Y_1|U) - I(V_1; Y_2|U), \\ I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U) \end{array} \right]. \tag{42}$$

Similarly, we can bound R_2 as

$$R_2 \leq \min \left[\begin{array}{l} I(V_2; Y_2|U) - I(V_2; Y_1|U), \\ I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U) \end{array} \right]. \tag{43}$$

Note that from (31) and (36) it follows that the joint distribution $P(u, v_1, v_2, x_1, x_2, y_1, y_2)$ factors as (7) for the interference channel. For the broadcast channel, we replace (X_1, X_2) by $X \triangleq X_Q$. Now, the joint distribution $P(u, v_1, v_2, x, y_1, y_2)$ factors as (11).

To consider the sum rate we let

$$\begin{aligned} \Delta_1 &= I(V_1; Y_1|U) - I(V_1; Y_2|U) \\ \Delta_2 &= I(V_2; Y_2|U) - I(V_2; Y_1|U) \\ \Theta_1 &= I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U) \\ \Theta_2 &= I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U). \end{aligned}$$

The bounds (42) and (43) imply the the following bounds on the sum rate:

$$R_1 + R_2 \leq \Delta_1 + \Delta_2, \tag{44}$$
$$R_1 + R_2 \leq \Theta_1 + \Theta_2 \tag{45}$$
$$R_1 + R_2 \leq \min[\Delta_1 + \Theta_2,\, \Delta_2 + \Theta_1] \tag{46}$$

where the bounds (44) and (45) are using either the first bounding approach (see Sec. IV-A) or the second bounding approach (see Sec. IV-B) only, and the bound (46) are based on both approaches. The following lemma illustrates that the combination sum rate bound (46) is indeed tighter than bounds (44) and (45).

Lemma 1:

$$\min[\Delta_1 + \Theta_2,\, \Delta_2 + \Theta_1] \leq \Delta_1 + \Delta_2 = \Theta_1 + \Theta_2.$$

Proof: We provide the proof in the Appendix. ■

It is interesting to further analyze the outer bound by comparing bounds (37) and (41). By assuming that δ and δ' converge to 0, the difference between these two bounds is

$$\begin{aligned} R_{1,\Delta} &\triangleq \Delta_1 - \Theta_1 \\ &= I(V_1; V_2|Y_2, U) - I(V_1; V_2|Y_1, U) \\ &= I(W_1; W_2|Y_2, U) - I(W_1; W_2|Y_1, U). \end{aligned} \tag{47}$$

We observe that, in general, the difference between bounds (37) and (41) is non-zero.

V. Inner Bound

A. Interference Channel with Confidential Messages

In this subsection we derive the achievable rate region for the interference channel. We prove that the region $\mathbb{R}_{\mathrm{IC}}(\pi_{\mathrm{IC-I}})$ is achievable. The coding structure for the IC-CM is illustrated in Fig. 6. We employ an auxiliary random variable U in the sense of Han-Kobayashi [21] and two equivocation codebooks (stochastic encoders), one for each message W_1 and W_2. Encoder t maps $\mathbf{v}_t$ into a channel input $\mathbf{x}_t$. More precisely, the random code generation is as follows.

Fix $P(u)$, $P(v_1|u)$ and $P(v_2|u)$, and

$$P(x_1, x_2|v_1, v_2) = P(x_1|v_1)P(x_2|v_2)$$

and let

$$R_1' \triangleq I(V_1; Y_2|V_2, U) - \epsilon_1 \tag{48}$$
$$R_2' \triangleq I(V_2; Y_1|V_1, U) - \epsilon_1 \tag{49}$$

where $\epsilon_1 > 0$ and ϵ_1 is small for sufficiently large n.

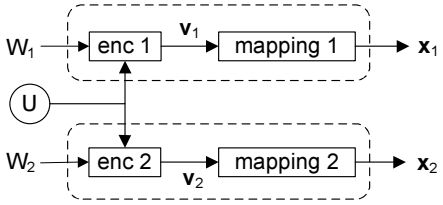


Fig. 6. Code construction for IC-CM

- [codebook generation] Randomly generate a typical sequence $\mathbf{u}$ with probability

$$P(\mathbf{u}) = \prod_{i=1}^{n} P(u_i),$$

and assume that both transmitters and receivers know the time-sharing sequence $\mathbf{u}$.
For transmitter t, $t = 1, 2$, generate $Q_t = 2^{n(R_t + R'_t)}$ independent sequences $\mathbf{v}_t$ each with probability

$$P(\mathbf{v}_t|\mathbf{u}) = \prod_{i=1}^{n} P(v_{t,i}|u_i)$$

and labeled as

$$\mathbf{v}_t(w_t, k_t),\ w_t \in \{1, \ldots, M_t\},\ k_t \in \{1, \ldots, M'_t\} \quad (50)$$

where $M_t = 2^{nR_t}$ and $M'_t = 2^{nR'_t}$. Without loss of generality, M_t, M'_t, and Q_t are assumed to be integers. Let

$$\mathcal{C}_t \triangleq \left\{\mathbf{v}_t(w_t, k_t),\ \text{for all } (w_t, k_t)\right\}$$

be the codebook of Transmitter t. Its w_t-th sub-codebook (bin)

$$\mathcal{C}_t(w_t) \triangleq \left\{\mathbf{v}_t(w_t, k_t),\ \text{for } k_t = 1, \ldots, M'_t\right\}$$

follows the partitioning in (50).
- [encoding] To send a message pair

$$(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2,$$

each transmitter employs a stochastic encoder. Encoder t randomly chooses an element $\mathbf{v}_t(w_t, k_t)$ from the sub-codebook $\mathcal{C}_t(w_t)$. Transmitters generate the channel input sequences based on respective mappings $P(x_1|v_1)$ and $P(x_2|v_2)$.
- [decoding] Given a typical sequence $\mathbf{u}$, let $A_\epsilon^{(n)}(P_{V_t,Y_t|U})$ denote the set of jointly typical sequences $\mathbf{v}_t$ and $\mathbf{y}_t$ with respect to $P(v_t, y_t|u)$ [5]. Decoder t chooses w_t so that

$$(\mathbf{v}_t(w_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(P_{V_t,Y_t|U})$$

when such w_t exists and and is unique; otherwise, an error is declared.

1) Error Probability Analysis: To bound the probability of error, we define the event

$$E_t(w_t, k_t) \triangleq \{(\mathbf{v}_t(w_t, k_t), \mathbf{y}_t|\mathbf{u}) \in A_\epsilon^{(n)}(P_{V_t,Y_t|U})\}.$$

Without loss of generality, we can assume that transmitter 1 sends the message $w_1 = 1$ associated with the codeword $\mathbf{v}_1(1, 1)$, and define the corresponding event

$$K_1 \triangleq \{\mathbf{v}_1(1, 1) \text{ sent}\}.$$

The union bound on the error probability of receiver 1 is as follows

$$\begin{aligned} P_{e,1}^{(n)} &\le P\left\{\bigcap_{k_1} E_1^c(1, k_1)\Big|K_1\right\} + \sum_{w_1 \ne 1,\, k_1} P\{E_1(w_1, k_1)|K_1\} \\ &\le P\{E_1^c(1, 1)|K_1\} + \sum_{w_1 \ne 1,\, k_1} P\{E_1(w_1, k_1)|K_1\} \end{aligned}$$

where $E_1^c(1, k_1)$ denotes the event

$$\{(\mathbf{v}_1(1, k_1), \mathbf{y}_1) \notin A_\epsilon^{(n)}(P_{V_1,Y_1|U})\}.$$

Following the joint asymptotic equipartition property (AEP) [5], we have

$$P\{E_1^c(1, 1)|K_1\} \le \epsilon,$$

and, for $w_1 \ne 1$,

$$P\{E_1(w_1, k_1)|K_1\} \le 2^{-n[I(V_1;Y_1|U)-\epsilon]}.$$

Hence, we can bound the probability of error as

$$\begin{aligned} P_{e,1}^{(n)} &\le \epsilon + Q_1 2^{-n[I(V_1;Y_1|U)-\epsilon]} \\ &= \epsilon + 2^{n(R_1+R'_1)}\, 2^{-n[I(V_1;Y_1|U)-\epsilon]} \end{aligned}$$

So, if

$$R_1 + R'_1 < I(V_1; Y_1|U),$$

then for any $\epsilon_0 > 0$, $P_{e,1}^{(n)} \le \epsilon_0$ for sufficiently large n. Similarly, for receiver 2, if

$$R_2 + R'_2 < I(V_2; Y_2|U),$$

then $P_{e,2}^{(n)} \le \epsilon_0$ for sufficiently large n. Hence, $P_e^{(n)} \le \epsilon_0$ as long as the rate pair $(R_1, R_2) \in \mathbb{R}_{\mathrm{IC}}(\pi_{\mathrm{IC-I}})$.

2) Equivocation Calculation: To show that (5a) holds, we consider the following equivocation lower bound

$$H(W_1|\mathbf{Y}_2) \ge H(W_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}) \quad (51)$$

where inequality (51) is due to the fact that conditioning reduces entropy. By applying the entropy chain rule [5], (51) can be expanded as follows

$$\begin{aligned} &H(W_1|\mathbf{Y}_2) \\ &\quad \ge H(W_1, \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) - H(\mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) \\ &\quad = H(W_1, \mathbf{V}_1, \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) \\ &\qquad - H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) - H(\mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) \\ &\quad = H(W_1, \mathbf{V}_1|\mathbf{V}_2, \mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) \\ &\qquad - H(\mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) + H(\mathbf{Y}_2|\mathbf{V}_1, \mathbf{V}_2, \mathbf{U}, W_1). \quad (52) \end{aligned}$$

Based on functional dependence graphs [27] and the random code construction, we can show that the following is a Markov chain

$$W_1 \to (\mathbf{V}_1, \mathbf{V}_2, \mathbf{U}) \to \mathbf{Y}_2$$

which yields

$$I(W_1; \mathbf{Y}_2|\mathbf{V}_1, \mathbf{V}_2, \mathbf{U}) = 0. \quad (53)$$

Hence, by using (52) and (53), we obtain

$$\begin{aligned} H(W_1|\mathbf{Y}_2) &\geq H(W_1,\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\quad - H(\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) + H(\mathbf{Y}_2|\mathbf{V}_1,\mathbf{V}_2,\mathbf{U}) \\ &= H(W_1,\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\quad - I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \\ &\geq H(\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\quad - I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}). \end{aligned} \tag{54}$$

We consider the first term in (54). Note that given $\mathbf{U}=\mathbf{u}$, $\mathbf{V}_1$ and $\mathbf{V}_2$ are independent and $\mathbf{V}_1$ has Q_1 possible values with equal probability. Hence,

$$\begin{aligned} H(\mathbf{V}_1|\mathbf{U},\mathbf{V}_2) &= H(\mathbf{V}_1|\mathbf{U}) \\ &= \log Q_1 \\ &= n(R_1+R_1'). \end{aligned} \tag{55}$$

We next show that $H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \leq n\epsilon_2$, where ϵ_2 is small for sufficiently large n. In order to calculate the conditional entropy $H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)$, we consider the following situation. We fix $W_1=w_1$, and assume that transmitter 1 transmits a codeword $\mathbf{v}_1(w_1,k_1)\in\mathcal{C}_1(w_1)$, for $1\leq k_1\leq M_1'$, and that receiver 2 knows the sequences $\mathbf{V}_2=\mathbf{v}_2$ and $\mathbf{U}=\mathbf{u}$. Given index $W_1=w_1$, receiver 2 decodes the codeword $\mathbf{v}_1(w_1,k_1)$ based on the received sequence $\mathbf{y}_2$. Let $\lambda(w_1)$ denote the average probability of error of decoding the index k_1 at receiver 2. Based on joint typicality [5, Chapter 8], we have the following lemma.

Lemma 2: $\lambda(w_1)\leq\epsilon_0$ for sufficiently large n.

Proof: We provide the proof in the Appendix. ∎

Fano's inequality implies that

$$\begin{aligned} \frac{1}{n}H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1=w_1) &\leq \frac{1}{n}[1+\lambda(w_1)\log M_1'] \\ &\leq \frac{1}{n}+\epsilon_0 I(V_1;Y_2|U) \\ &\triangleq \epsilon_2 \end{aligned} \tag{56}$$

where the second inequality follows from Lemma 2 and (48). Consequently,

$$\begin{aligned} &\frac{1}{n}H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\quad= \frac{1}{n}\sum_{w_1\in\mathcal{W}_1} P(W_1=w_1)H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1=w_1) \\ &\quad\leq \epsilon_2. \end{aligned} \tag{57}$$

Finally, the third term in (54) can be bounded based on the following lemma.

Lemma 3:

$$I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \leq nI(V_1;Y_2|V_2,U)+n\epsilon_3 \tag{58}$$

where ϵ_3 is small for sufficiently large n.

Proof: We provide the proof in the Appendix. ∎

By using (55), (57), and (58), we can rewrite (54) as

$$\frac{1}{n}H(W_1|\mathbf{Y}_2) \geq R_1+R_1'-I(V_1;Y_2|V_2,U)-\epsilon_2-\epsilon_3.$$

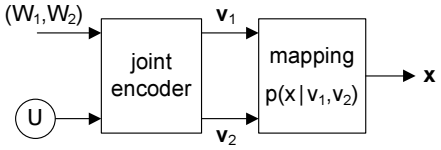


Fig. 7. Code construction for BC-CM

By the definition of R_1' (48), we have

$$R_1-\frac{1}{n}H(W_1|\mathbf{Y}_2,\mathbf{X}_2,W_2)\leq\epsilon_4 \tag{59}$$

where $\epsilon_4\triangleq\epsilon_1+\epsilon_2+\epsilon_3$, and, thus, the security condition (5a) is satisfied. Following the same approach, we can prove that (5b) is satisfied.

B. Broadcast Channel with Confidential Messages

We next prove Theorem 4 based on the *double-binning* scheme which combines the *Gel'fand-Pinsker binning* [23] and the *random binning*. In this subsection we redefine the parameters R_1, R_2, R_1', R_2', Q_1, Q_2, M_1, and M_2. The coding structure for the BC-CM is shown in Fig. 7. We employ a joint encoder to generate two equivocation codewords $\mathbf{v}_1$ and $\mathbf{v}_2$, one for each message W_1 and W_2. The equivocation codewords are mapped into the channel input $\mathbf{x}$. The details of random code generation are as follows.

We fix $P(u)$, $P(v_1|u)$ and $P(v_2|u)$, as well as $P(x|v_1,v_2)$. Let $0\leq\alpha\leq 1$,

$$\begin{aligned} R_1' &\triangleq I(V_1;Y_2|V_2,U)-\epsilon_1' \\ R_2' &\triangleq I(V_2;Y_1|V_1,U)-\epsilon_1' \end{aligned} \tag{60}$$

and

$$R^\dagger \triangleq I(V_1;V_2|U)+\epsilon_1' \tag{61}$$

where $\epsilon_1'>0$ and ϵ_1' is small for sufficiently large n.

- [codebook generation] We generate randomly a typical sequence $\mathbf{u}$ with probability

  $$P(\mathbf{u})=\prod_{i=1}^{n}P(u_i)$$

  and assume that both the transmitter and the receivers know the sequence $\mathbf{u}$.
  We generate $Q_t=2^{n(R_t+R_t'+R^\dagger)}$ independent sequences $\mathbf{v}_t$ each with probability

  $$P(\mathbf{v}_t|\mathbf{u})=\prod_{i=1}^{n}P(v_{t,i}|u_i)$$

  and label them

  $$\begin{aligned} &\mathbf{v}_t(w_t,s_t,k_t),\quad w_t\in\{1,\ldots,M_t\},\ s_t\in\{1,\ldots,J_t\}, \\ &\qquad\text{and } k_t\in\{1,\ldots,G_t\}. \end{aligned} \tag{62}$$

  where $M_t=2^{nR_t}$, $J_t=2^{nR_t'}$, and $G_t=2^{nR^\dagger}$. Without loss of generality Q_t, M_t, J_t, and G_t are considered to be integers. Let

  $$\mathcal{C}_t\triangleq\left\{\mathbf{v}_t(w_t,s_t,k_t),\ \text{for all } (w_t,s_t,k_t)\right\}$$

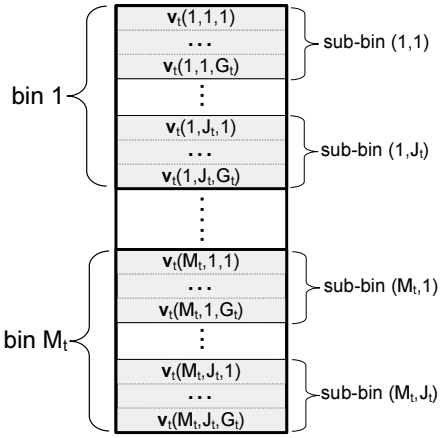


Fig. 8. Double binning

denote the transmitter t codebook. Based on the labeling in (62), the codebook $\mathcal{C}_t$ is partitioned into M_t bins, and the w_t-th bin is

$$\mathcal{C}_t(w_t) \triangleq \{\mathbf{v}_t(w_t, s_t, k_t), \text{ for } s_t \in \{1,\ldots,J_t\} \text{ and } k_t \in \{1,\ldots,G_t\}.$$

Furthermore, each bin $\mathcal{C}_t(w_t)$ is divided into J_t sub-bins, and the (w_t, s_t)-th sub-bin is

$$\mathcal{C}_t(w_t, s_t) \triangleq \big\{\mathbf{v}_t(w_t, s_t, k_t), \text{ for } k_t \in \{1,\ldots,G_t\}\big\}.$$

The double binning structure for $\mathbf{v}_t$ sequences is shown in Fig. 8.

- [encoding] To send the message pair $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, the transmitter employs a stochastic encoder. We randomly choose a sub-bin $\mathcal{C}_t(w_t, s_t)$ from the bin $\mathcal{C}_t(w_t)$, for $t = 1, 2$. Next, we select a pair (k_1, k_2) so that
$$\big(\mathbf{v}_1(w_1, s_1, k_1), \mathbf{v}_2(w_2, s_2, k_2)\big) \in A_\epsilon^{(n)}(P_{V_1,V_2|U}),$$
where $A_\epsilon^{(n)}(P_{V_1,V_2|U})$ denotes, for a given typical sequence $\mathbf{u}$, the set of jointly typical sequences $\mathbf{v}_1$ and $\mathbf{v}_2$ with respect to $P(v_1, v_2|u)$. If there are more than one such pairs, then we randomly select one. We generate the channel input sequence $\mathbf{x}$ according to the mapping $P(x|v_1, v_2)$.
- [decoding] For a given typical sequence $\mathbf{u}$, let $A_\epsilon^{(n)}(P_{V_t,Y_t|U})$ denote the set of jointly typical sequences $\mathbf{v}_t$ and $\mathbf{y}_t$ with respect to $P(v_t, y_t|u)$. Decoder t chooses w_t so that $(\mathbf{v}_t(w_t, s_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(P_{V_t,Y_t|U})$ if such w_t exists and is unique; otherwise, an error is declared.

1) Error Probability Analysis: Without loss of generality, we assume that the message pair is $(w_1 = 1, w_2 = 1)$ and that $s_1 = s_2 = 1$. First, we consider the error event T that the encoder can not find an appropriate jointly typical pair, i.e.,

$$T \triangleq \{\big(\mathbf{v}_1(1,1,k_1), \mathbf{v}_2(1,1,k_2)\big) \notin A_\epsilon^{(n)}(P_{V_1,V_2|U}), \text{ for } s_t = 1,\ldots,J_t,\ k_t = 1,\ldots,G_t, \text{ and } t = 1,2\}.$$

The definition of $R^\dagger$ in (61) implies that

$$R^\dagger > I(V_1; V_2|U). \tag{63}$$

Hence, following the approach of [28], we have that

$$P\{T\} \le \delta_3 \tag{64}$$

where $\delta_3 > 0$ and δ_3 is small for sufficiently large n. In other words, the encoding is successful with probability close to 1 as long as n is large.

In the following, we assume that $(v_1(1,1,1), v_2(1,1,1))$ is sent and define the event

$$K_2 \triangleq \{(\mathbf{v}_1(1,1,1), \mathbf{v}_2(1,1,1)) \in A_\epsilon^{(n)}(P_{V_1,V_2|U})\}.$$

Now, the error probability at receiver 1 is bounded as follows

$$\begin{aligned} P_{e,1}^{(n)} &\le P\{T\} + (1 - P\{T\})\left[P\left\{\bigcap_{s_1,k_1} E_1^c(1, s_1, k_1)\Big|K_2\right\}\right. \\ &\qquad \left. + \sum_{w_1\neq 1}\sum_{s_1,k_1} P\{E_1(w_1, s_1, k_1)|K_2\}\right] \\ &\le P\{T\} + P\{E_1^c(1,1,1)|K_2\} \\ &\qquad + \sum_{w_1\neq 1}\sum_{s_1,k_1} P\{E_1(w_1, s_1, k_1)|K_2\} \end{aligned}$$

where

$$E_t(w_t, s_t, k_t) = \{(\mathbf{v}_t(w_t, s_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(P_{V_t,Y_t|U})\}.$$

Joint typicality [5, Chapter 14] implies that

$$\begin{aligned} &P\{E_1^c(1,1,1)|K_2\} \le \epsilon, \\ &P\{E_1(w_1, s_1, k_1)|K_2\} \le 2^{-n[I(V_1;Y_1|U)-\epsilon]} \quad \text{for } w_1 \neq 1. \end{aligned}$$

Hence, we can bound the probability of error as

$$\begin{aligned} P_{e,1}^{(n)} &\le \delta_3 + \epsilon + Q_1 2^{-n[I(V_1;Y_1|U)-\epsilon]} \\ &= \delta_3 + \epsilon + 2^{n(R_1+R_1'+R^\dagger)}\, 2^{-n[I(V_1;Y_1|U)-\epsilon]} \end{aligned} \tag{65}$$

So, if

$$R_1 + R_1' + R^\dagger < I(V_1; Y_1|U), \tag{66}$$

then for any $\epsilon_0 > 0$, $P_{e,1}^{(n)} \le \epsilon_0$ for sufficiently large n. Similarly, for receiver 2, if

$$R_2 + R_2' + R^\dagger < I(V_2; Y_2|U), \tag{67}$$

then $P_{e,2}^{(n)} \le \epsilon_0$ for sufficiently large n. Hence, (2), (60), (61), (66), and (67) imply that $P_e^{(n)} \le \epsilon_0$ as long as the rate pair $(R_1, R_2) \in \mathbb{R}_{\mathrm{BC}}(\pi_{\mathrm{BC}})$.

2) Equivocation Calculation: We next prove that the secrecy requirement (5a) holds for BC-CM. Following the same approach as (51)–(54), we have

$$\begin{aligned} H(W_1|\mathbf{Y}_2) \ge H(\mathbf{V}_1|\mathbf{V}_2, \mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) \\ - I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}). \end{aligned} \tag{68}$$

Consider the first term in (68)

$$H(\mathbf{V}_1|\mathbf{U}, \mathbf{V}_2) = H(\mathbf{V}_1|\mathbf{U}) - I(\mathbf{V}_1; \mathbf{V}_2|\mathbf{U}).$$

Note that given $\mathbf{U} = \mathbf{u}$, $\mathbf{V}_1$ attains Q_1 possible values with equal probability. Hence, we have $H(\mathbf{V}_1|\mathbf{U}) = \log Q_1$. Using the same approach as in Lemma 3, we can obtain

$$I(\mathbf{V}_1; \mathbf{V}_2|\mathbf{U}) \le nI(V_1; V_2|U) + n\epsilon_2'. \tag{69}$$

Hence, by the definition of $R^\dagger$ in (61), we have

$$\begin{aligned} H(\mathbf{V}_1|\mathbf{U},\mathbf{V}_2) &= \log Q_1 - I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U}) \\ &\geq n(R_1 + R_1' + R^\dagger) - nI(V_1;V_2|U) - n\epsilon_2' \\ &\geq n(R_1 + R_1' - \epsilon_2'). \end{aligned} \tag{70}$$

Following joint typicality [5], (57) implies

$$H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \leq n\epsilon_3'$$

where ϵ_3' is small for sufficiently large n. Applying Lemma 3, the third term in (68) can be bounded as

$$\begin{aligned} I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) &\leq nI(V_1;Y_2|V_2,U) + n\epsilon_4' \\ &= n(R_1' + \epsilon_1' + \epsilon_4') \end{aligned} \tag{71}$$

where ϵ_4' is small for sufficiently large n and the equality (71) follows from the definition (60). Hence, by using (69), (70), and (71), we can rewrite (68) as

$$\frac{1}{n}H(W_1|\mathbf{Y}_2) \geq R_1 - \epsilon_5'$$

where $\epsilon_5' \triangleq \epsilon_1' + \epsilon_2' + \epsilon_3' + \epsilon_4'$, and thus the security condition (5a) is satisfied. Following the same approach, we can prove that (5b) also holds.

VI. Conclusion

We derived the outer and the inner bounds on the capacity of the interference and broadcast channels with confidential messages. The obtained results offer insights into the two communication problems. The difference in the outer bound reflects the fact that the joint encoding at the transmitter can only be performed in the BC-CM whereas in the IC-CM, encoders offer independent channel inputs. The achievability proof suggests the code construction appropriate for these channel. We presented a special case of IC-CM for which the two bounds meet to describe the capacity region. We proposed and compared several transmission schemes for Gaussian interference channels under information-theoretic secrecy. In particular, the encoding scheme in which transmitters dedicate some of their power to create artificial noise was shown to outperform both time-sharing and simultaneous transmission of messages sent with the optimal power. However, constructing practical wiretap codes that can achieve the derived rates is a challenging problem. Code constructions for a binary-input Gaussian wiretap channel have recently been proposed in [29].

Appendix

Proof: **(Lemma 1)** By the definition of Δ_1, we have

$$\begin{aligned} \Delta_1 &= I(V_1;Y_1|U) - I(V_1;Y_2|U) \\ &= I(V_1,V_2;Y_1|U) - I(V_2;Y_1|V_1,U) \\ &\quad - I(V_1,V_2;Y_2|U) + I(V_2;Y_2|V_1,U). \end{aligned} \tag{72}$$

Similarly,

$$\begin{aligned} \Delta_2 &= I(V_2;Y_2|U) - I(V_2;Y_1|U) \\ &= I(V_1,V_2;Y_2|U) - I(V_1;Y_2|V_2,U) \\ &\quad - I(V_1,V_2;Y_2|U) + I(V_1;Y_1|V_2,U). \end{aligned} \tag{73}$$

(72) and (73) imply that

$$\begin{aligned} \Delta_1 + \Delta_2 &= -I(V_2;Y_1|V_1,U) + I(V_2;Y_2|V_1,U) \\ &\quad - I(V_1;Y_2|V_2,U) + I(V_1;Y_1|V_2,U) \\ &= \Theta_2 + \Theta_1. \end{aligned} \tag{74}$$

Note that

$$\begin{aligned} 2(\Delta_1 + \Delta_2) &= 2(\Theta_1 + \Theta_2) \\ &= (\Delta_1 + \Theta_2) + (\Delta_2 + \Theta_1) \end{aligned}$$

Hence,

$$\min[\Delta_1 + \Theta_2,\ \Delta_2 + \Theta_1] \leq \Delta_1 + \Delta_2 = \Theta_1 + \Theta_2.$$

We have the derived results. ■

Proof: **(Lemma 2)** For a given typical sequence pair $(\mathbf{v}_2,\mathbf{u})$, let $A_\epsilon^{(n)}(P_{V_1,Y_2|V_2,U})$ denote the set of jointly typical sequences $\mathbf{v}_1$ and $\mathbf{y}_2$ with respect to $P(v_1,y_2|v_2,u)$. For a given $W_1 = w_1$, decoder 2 chooses k_1 so that

$$(\mathbf{v}_1(w_1,k_1),\mathbf{y}_2) \in A_\epsilon^{(n)}(P_{V_1,Y_2|V_2,U})$$

if such k_1 exists and is unique; otherwise, an error is declared. Define the event

$$\hat{E}(k_1) = \{(\mathbf{v}_1(w_1,k_1),\mathbf{y}_2) \in A_\epsilon^{(n)}(P_{V_1,Y_2|V_2,U})\}.$$

Without loss of generality, we assume that $\mathbf{v}_1(w_1,k_1=1)$ was sent, and define the event

$$\hat{K}_1 = \big\{\mathbf{v}_1(w_1,1) \text{ sent}\big\}.$$

Hence

$$\lambda(w_1) \leq P\{\hat{E}^c(k_1=1)|\hat{K}_1\} + \sum_{k_1\neq 1} P\{\hat{E}(k_1)|\hat{K}_1\}$$

where $\hat{E}^c(k_1=1)$ denotes the event

$$\{(\mathbf{v}_1(w_1,1),\mathbf{y}_2) \notin A_\epsilon^{(n)}(P_{V_1,Y_2|V_2,U})\}.$$

Following the joint AEP [5], we have

$$P\{\hat{E}^c(k_1=1)|\hat{K}_1\} \leq \epsilon,$$

and, for $k_1 \neq 1$,

$$P\{\hat{E}(k_1)|\hat{K}_1\} \leq 2^{-n[I(V_1;Y_2|V_2,U)-\epsilon]}.$$

Now, we can bound the probability of error as

$$\begin{aligned} \lambda(w_1) &\leq \epsilon + M_1' 2^{-n[I(V_1;Y_2|V_2,U)-\epsilon]} \\ &\leq \epsilon + 2^{nR_1'}\, 2^{-n[I(V_1;Y_2|V_2,U)-\epsilon]}. \end{aligned}$$

Note that $R_1' = I(V_1;Y_2|V_2,U) - \epsilon_1$. Hence, by choosing $\epsilon_1 > \epsilon$, we have

$$\lambda(w_1) \leq \epsilon_0$$

where ϵ_0 is small for sufficiently large n. ■

Proof: **(Lemma 3)** Let $A_\epsilon^{(n)}(P_{U,V_1,V_2,Y_2})$ denote the set of typical sequences $(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)$ with respect to $P(u,v_1,v_2,y_2)$, and

$$\mu(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2) = \begin{cases} 1, & (\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2) \notin A_\epsilon^{(n)}(P_{U,V_1,V_2,Y_2}) \\ 0, & \text{otherwise} \end{cases}$$

be the corresponding indicator function.

We expand $I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U})$ as

$$\begin{aligned} I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) &\le I(\mathbf{V}_1,\mu;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \\ &= I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu)+I(\mu;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \\ &= \sum_{j=0}^{1} P(\mu=j) I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=j) \\ &\quad + I(\mu;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \end{aligned} \tag{75}$$

Note that

$$\begin{aligned} &P(\mu=1) I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=1) \\ &\quad \le nP\big[(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\notin A_\epsilon^{(n)}(P_{U,V_1,V_2,Y_2})\big]\log|\mathcal{Y}_2| \\ &\quad \le n\epsilon\log|\mathcal{Y}_2|, \end{aligned} \tag{76}$$

and

$$I(\mu;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \le H(\mu) \le 1. \tag{77}$$

We only consider the term $P(\mu=0)I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=0)$. Following the sequence joint typicality properties [5], we have

$$\begin{aligned} &P(\mu=0) I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=0) \\ &\quad \le I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=0) \\ &\quad = \sum_{(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\in A_\epsilon^{(n)}} P(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)[\log P(\mathbf{v}_1,\mathbf{y}_2|\mathbf{v}_2,\mathbf{u}) \\ &\qquad - \log P(\mathbf{y}_2|\mathbf{v}_2,\mathbf{u}) - \log P(\mathbf{v}_1|\mathbf{v}_2,\mathbf{u})] \\ &\quad \le n[H(Y_2|V_2,U)+H(V_1|V_2,U) \\ &\qquad - H(V_1,Y_2|V_2,U)+3\epsilon] \\ &\quad = nI(V_1;Y_2|V_2,U)+3\epsilon. \end{aligned} \tag{78}$$

Combining (75), (76), (77), and (78), we have the desired result

$$\begin{aligned} I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2\mathbf{U}) &\le nI(V_1;Y_2|V_2,U) \\ &\quad + n\Big(\epsilon\log|\mathcal{Y}_2|+3\epsilon+\frac{1}{n}\Big) \\ &= nI(V_1;Y_2|V_2,U)+n\epsilon_3 \end{aligned}$$

where

$$\epsilon_3 \triangleq \epsilon\log|\mathcal{Y}_2|+3\epsilon+\frac{1}{n}.$$

■

Proof: **(Theorem 5)** Since the switch channel is a special case of the interference channel, we focus on the outer bound (9) and the inner bound (10) and prove that

$$\mathbb{R}_{\mathrm{O}}(\pi_{\mathrm{IC-O}}) = \mathbb{R}_{\mathrm{IC}}(\pi_{\mathrm{IC-I}})$$

for the SC-CM case.

We note that the distribution $\pi_{\mathrm{IC-I}}$ implies that, for a given U, auxiliary random variables V_1 and V_2 are independent, but this may not hold for the distribution $\pi_{\mathrm{IC-O}}$. Hence, we need to first show that the condition

$$I(V_1;V_2|U)=0 \tag{79}$$

holds in the outer bound for SC-CM. Furthermore, if

$$I(V_1;V_2|Y_2,U)=0 \tag{80}$$

also holds in the outer bound for SC-CM, then we have

$$\begin{aligned} I(V_1;Y_2|V_2,U) &= I(V_1;Y_2|U)+I(V_1;V_2|Y_2,U) \\ &\quad - I(V_1;V_2|U) \\ &= I(V_1;Y_2|U), \\ I(V_2;Y_2|V_1,U) &= I(V_2;Y_2|U)+I(V_1;V_2|Y_2,U) \\ &\quad - I(V_1;V_2|U) \\ &= I(V_2;Y_2|U), \end{aligned} \tag{81}$$

that is, the outer bound (9) meets the inner bound (10).

Now, we prove that conditions (79) and (80) holds in the outer bound for SC-CM. By definitions (31) and (36), we need to show that

$$I(W_1;W_2|U_i)=0 \tag{82}$$

$$I(W_1;W_2|U_i,Y_{2,i})=0 \tag{83}$$

where $U_i=\{\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1}\}$. We first prove the equality (82). Following the switch output definition (19), we have

$$\{\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1}\}=\{\mathbf{Z}_1^{i-1},\tilde{\mathbf{Z}}_2^{i+1},\mathbf{S}_1^{i-1},\tilde{\mathbf{S}}_2^{i+1}\} \tag{84}$$

and hence,

$$I(W_1;W_2|U_i) \tag{85}$$

$$\begin{aligned} &= I(W_1;W_2|\mathbf{Z}_1^{i-1},\tilde{\mathbf{Z}}_2^{i+1},\mathbf{S}_1^{i-1},\tilde{\mathbf{S}}_2^{i+1}) \\ &= \sum_{\mathbf{s}_1^{i-1}}\sum_{\tilde{\mathbf{s}}_2^{i+1}} P(\mathbf{S}_1^{i-1}=\mathbf{s}_1^{i-1},\tilde{\mathbf{S}}_2^{i+1}=\tilde{\mathbf{s}}_2^{i+1}) \\ &\qquad I(W_1;W_2|\mathbf{Z}_1^{i-1},\tilde{\mathbf{Z}}_2^{i+1},\mathbf{s}_1^{i-1},\tilde{\mathbf{s}}_2^{i+1}) \\ &= \sum_{\mathbf{s}_1^{i-1}}\sum_{\tilde{\mathbf{s}}_2^{i+1}}\left[\prod_{j=1}^{i-1}P(S_{1,j}=s_{1,j})\prod_{k=i+1}^{n}P(S_{2,k}=s_{2,k})\right] \\ &\qquad I(W_1;W_2|\mathbf{Z}_1^{i-1},\tilde{\mathbf{Z}}_2^{i+1},\mathbf{s}_1^{i-1},\tilde{\mathbf{s}}_2^{i+1}). \end{aligned} \tag{86}$$

Now, for a given $s_{t,i}$, the switch channel model (18) implies that $z_{t,i}$ only depend on the channel input $x_{s_{t,i},i}$. By using functional dependence graphs [27], we can easily verify that

$$I(W_1;W_2|\mathbf{Z}_1^{i-1},\tilde{\mathbf{Z}}_2^{i+1},\mathbf{s}_1^{i-1},\tilde{\mathbf{s}}_2^{i+1})=0$$

for fixed switch state information $\mathbf{s}_1^{i-1}$ and $\tilde{\mathbf{s}}_2^{i+1}$. Hence, (86) implies that $I(W_1;W_2|U_i)=0$. Following the same approach, we can prove the equality (83). Therefore, we have the desired result. ■

ACKNOWLEDGMENT

The authors would like to thank Professor Shlomo Shamai (Shitz) of the Technion, Gerhard Kramer, Bell Labs, Alcatel-Lucent, and Chandra Nair, Chinese University of Hong Kong for their useful comments about the proof of the outer bound.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006, pp. 952–956.

[4] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006, pp. 957–961.
[5] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley Sons, Inc., 1991.
[6] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. on Inf. Theory*, submitted (under revision), April 2006. [Online]. Available: http://www.arxiv.org/PS$_$cache/cs/pdf/0605/0605014.pdf
[7] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," http://arxiv.org/abs/cs/0605028, 2006.
[8] ——, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006.
[9] ——, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. 44th Annual Allerton Conference Communication, Control, and Computing*, Monticello, IL, Sep. 2006.
[10] ——, "The multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Proc. Information Theory and Application Workshop, ITA*, San Diego, CA, Jan. 2007.
[11] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sept. 2001, pp. 87–89.
[12] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. on Inf. Theory*, submitted, Dec 2006. [Online]. Available: http://www.ece.osu.edu/$\thicksim$helgamal/relay-eavesdropper.pdf
[13] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai(Shitz), and S. Verdú, "Cognitive interference channels with confidential messages," in *Proc. 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sep. 2007.
[14] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, Jul. 2006, pp. 356–360.
[15] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proc. 44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sep. 2006.
[16] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007, pp. 1306–1310.
[17] Z. Li, R. D. Yates, and W. Trappe, "Secure communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007, pp. 1296–1300.
[18] X. Tang, R. Liu, and P. Spasojevic, "An achievable secrecy throughput of hybrid-arq protocols for block fading channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007, pp. 1311–1315.
[19] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. on Inf. Theory*, vol. 25, no. 1, pp. 306–311, May 1979.
[20] A. B. Carleial, "Interference channels," *IEEE Trans. on Inf. Theory*, vol. 24, no. 1, p. 60, Jan. 1978.
[21] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. on Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.
[22] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT, Lecture Notes in Computer Science*, 2000, pp. 351–368.
[23] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problemy Peredachi Informatsii*, vol. 9, no. 1, pp. 19–31, 1980.
[24] R. Liu and H. V. Poor, "Multiple antenna secure broadcast over wireless networks," in *Proc. First International Workshop on Information Theory for Sensor Networks*, Santa Fe, NM, June 18-20, 2007, pp. 125–139.
[25] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Multi-terminal communications with confidential messages," in *Proc. Information Theory and Application Workshop, ITA*, San Diego, CA, Jan. 2007.
[26] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[27] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Trans. on Inf. Theory*, vol. 49, pp. 4–21, Jan. 2003.
[28] A. El Gamal and E. Van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. on Inf. Theory*, vol. 27, pp. 120–122, Jul. 1980.
[29] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Information Theory Workshop (ITW)*, Lake Tahoe, California, September 2-6, 2007, pp. 337 – 342.